REMARKS

Claims 21 and 31 are amended. Claims 21-31, as amended, remain in the application. No new matter is added by the amendments to the Claims.

The Rejections:

In the Final Office Action dated July 27, 2007, the Examiner rejected Claims 21-31 under 35 U.S.C. 103(a) as being unpatentable over Kanevsky, et al. (US 6,421,453) and further in view of An, et al. (US 6,715,073).

As per Claim 21, the Examiner stated that:

Kanevsky discloses a method of initiating a procedure within a building comprising the steps of:

a. defining at least one initiating event for the procedure which event does not involve a person arriving at the building [col. 3, lines 29-37 and col. 4, lines 61-67; The claimed defining an initiating even that does not involve a person arriving at the building can broadly interpret as classifying or identifying an event occurring remotely such as a service via the Internet or to another computer of different location. Kanevsky discloses performing a certain act such as access to a service or a facility refers to an initiating event for the procedure (col. 12, lines 42-45) where access to a service can obviously be the initiating event that does not involve a person arriving at the building and remote transactions between a user and a computer (col. 1, lines 26-27).]

b. defining at least one requirement for the procedure; [col. 8, lines 58-67 and col. 9, lines 24-29; a requirement can be interpreted as biometrics, certain gesture pins particular to a service, security task(s), or level of security.]

c. defining at least one person to be authorized to perform the procedure; [col. 1, lines 57-63 and col. 14, lines 42-54]

d. detecting the occurrence of the at least one initiating event; [col. 1, lines 65-67 and col. 9, lines 1-3; detecting the occurrence is when the person comes to the interacting system or interface area (col. 1, lines 16-22)]

e. generating a virtual key for the at least one based on the at least one requirement detecting the occurrence of the at least one initiating event and prior to the at least one person arriving at the building; [col. 17, lines 20-25 and col. 18, lines 47-52; the requirement for the procedure in generating the virtual key is the security task(s) where the desired level of security determines what type of gesture sequences (virtual key) are acceptable or where a high degree of security is required (col. 8, lines 58-67 and col. 9, lines 24-29) or according to the predetermined standards (col. 18, lines 59-63.]

f. transmitting virtual key to the at least one person; [col. 17, lines 5-7 and 59-60 and col. 18, lines 9-10 50-51]

g. detecting use of the virtual key; [col. 9, lines 64-66 and col. 16, lines 64-66]

h. checking the validity of the virtual key; and [col. 5, lines 39-43 and col. 12, lines 40-47]

i. initiating said procedure within the building if the validity check is positive. [col. 13, lines 55-60 and col. 15, lines 29-57; Kanevsky discloses the use of sensors to initiate a procedure.]

j. performing said steps a. through i. in an access control computer system associated with the building. [col. 5, lines 32-35 and col. 18, lines 50-51]

According to the Examiner, Kanevsky discloses a gesture pin or password as the claimed virtual key suggesting proof of possession (col. 5, lines 3-10) that is used to verify the person or user to gain access to the building or facilities (col. 5, lines 40-43 and col. 8, lines 23-40). Kanevsky discloses the passwords (gesture pins) are generated during an enrollment session where during enrollment session, gesture pins may be either predefined or provided to a user (col. 17, lines 5-7). Therefore, the gesture pin is the password being transmitted to a user for use to access the computer/facility/service and checking the validity of the gesture pin (col. 15, lines 41-47 and 18, lines 8-24). However, Kanevsky does not specifically disclose a password refers to a virtual key.

An, et al. is brought forth to teach a virtual key can also be considered as a password. An teaches organizations controls access for customers or users by registering user identification and passwords. That the password is a virtual key that authenticates a user (col. 1, lines 43-48 and

col. 2, lines 4-10). Thus, it would have been obvious for a person of ordinary skills in the art at the time of the invention to combine the teaching of the gesture pin or password as taught by Kanevsky with the teaching of a virtual key is also referred as a password as taught by An because both virtual keys and passwords has a common function which is for use to authenticate/authorize a user to gain access (An - col.1, lines 43-48 and col.2, lines 4-10).

As per Claim 22: See An on col. 1, lines 64 - col. 2, line 1; discusses a step of assigning an encrypted code to the virtual key.

As per Claim 23: See An on col. 2, lines 5-12; discusses the steps of adding a signature to the virtual key and identifying a recipient of the transmitted virtual key by the signature.

As per Claim 24: See Kanevsky on col. 1, lines 49-55; discusses defining different procedures for different initiating events.

As per Claim 25: See Kanevsky on col. 13, lines 59-62 and col. 29-53; discusses defining different requirements for different procedures.

As per Claim 26: See Kanevsky on col. 9, lines 25-27 and An on col. 1, lines 64 - col. 2, line 12; discusses transmitting different virtual keys to said person for different initiating events.

As per Claim 27: See Kanevsky on col. 17, lines 20-30; discusses storing said virtual key partially or completely.

As per Claim 28: See Kanevsky on col. 17, lines 20-30; discusses the steps of identifying the at least one person with biometrics characteristics.

As per Claim 29: Kanevsky discusses the method according to Claim 21, further comprising at least one of the steps of: initiating a control procedure of an elevator in the building; initiating a medical assistance procedure; initiating a building cleaning procedure; and initiating a guest reception procedure.

Kanevsky discloses classification involves the differentiation of multiple individuals attempting to interact with the system and a purpose of identifying the individuals from their respective commands (col. 1, lines 49-58 and col. 5, lines 3-17). Kanevsky discusses that it is desirable to implement an extension of the identification task where the individuals attempting to interface with the computer are ranked so that a higher ranking individual (i.e. supervisor) is allowed access over a lower ranked individual (i.e. data entry person) (col. 1, line 65 - col. 2, line

1). Further, Kanevsky discloses an apparatus/procedure for obtaining access to a computer/facility/service via the utilization of gesture pins (col. 15, lines 29-32). Thus, it would have been obvious the computer/facility/service is referring to initiating a variety of procedures (i.e. an elevator in a building, medical assistance, building cleaning procedure or guest reception) that includes security tasks for different users to access to different services/facilities.

As per Claim 30: See Kanevsky on col. 31, lines 63-64; discusses the step of transmitting the virtual key using wireless devices.

As per Claim 31, the Examiner stated that:

Kanevsky discloses a method of initiating a procedure within a building comprising the steps of:

a. defining at least one initiating event for the procedure which event does not involve a person arriving at the building; col. 3, lines 29-37 and col. 4, lines 61-67; The claimed defining an initiating even that does not involve a person arriving at the building can broadly interpret as classifying or identifying an event occurring remotely such as a service via the Internet or to another computer in another building of different geographic region. Kanevsky discloses performing a certain act or the security task(s) such as access to a service or a facility refers to an initiating event for the procedure (col. 12, lines 42-45) where access to a service can obviously be given as an event that does not involve a person arriving at the building remote transactions between a user and a computer (col. 1, lines 26-27).]

b. defining at least one of a security requirement and an availability requirement for the procedure; [col. 8, lines 58-67 and col. 9, lines 25-29; i.e. security task(s) or level of security]

c. defining at least one person to be authorized to perform the procedure; [col. 1, lines 57-63 and col. 14, lines 42-54]

d. detecting the occurrence of the at least one initiating event; [col. 1, lines 65-67 and col. 9, lines 1-3; detecting the occurrence is when the person comes to the interacting system or interface area (col. 1, lines 16-22)]

e. generating a virtual key for the at least one based on the at least one requirement detecting the occurrence of the at least one initiating event and prior to the at least one person arriving at the building; [col. 17, lines 20-25 and col. 18, lines 47-52; a requirement can be

interpreted as biometrics, certain gesture pins particular to a service, security task(s), or level of security. The security requirement for the procedure can broadly be given as the security task(s) where the desired level of security determines what type of gesture sequences (virtual key) are acceptable or where a high degree of security is required (col. 8, lines 58-67 and col. 9, lines 24-29).]

f. transmitting virtual key to the at least one person; [col. 17, lines 5-7 and 59-60 and col. 18, lines 9-10 and 30-32]

g. detecting use of the virtual key; [col. 9, lines 64-66 and col. 16, lines 64-66]

h. checking the validity of the virtual key; and [col. 5, lines 39-43 and col. 12, lines 40-47]

i. initiating said procedure within the building if the validity check is positive. [col. 13, lines 55-60 and col. 15, lines 29-57; Kanevsky discloses the use of sensors to initiate a procedure.]

j. performing said steps a. through i. in an access control computer system associated with the building. [col. 5, lines 32-35 and col. 18, lines 50-51]

The Examiner stated that Kanevsky discloses a gesture pin or password as the claimed virtual key suggesting proof of possession (col. 5, lines 3-10) that is used to verify the person or user to gain access to the building or facilities (col. 5, lines 40-43 and col. 8, lines 23-40). Kanevsky discloses the passwords (gesture pins) are generated during an enrollment session where during enrollment session, gesture pins may be either predefined or provided to a user (col. 17, lines 5-7). Therefore, the gesture pin is the password being transmitted to a user for use to access the computer/facility/service and checking the validity of the gesture pin (col. 15, lines 41-47 and 18, lines 8-24). However, Kanevsky does not specifically disclose a password refers to a virtual key.

An, et al. is brought forth to each a virtual key can also be considered as a password. An teaches organizations controls access for customers or users by registering user identification and passwords. That the password is a virtual key that authenticates a user (col. 1, lines 43-48 and col. 2, lines 4-10). Thus, it would have been obvious for a person of ordinary skills in the art at the time of the invention to combine the teaching of the gesture pin or password as taught by

Kanevsky with the teaching of a virtual key is also referred as a password as taught by An because both virtual keys and passwords has a common function which is for use to authenticate/authorize a user to gain access (An – col. 1, lines 43-48 and col. 2, lines 4-10).

The Examiner stated that Applicant's arguments filed 6/19/2007 have been fully considered but they are not persuasive. According to the Examiner, Kanevsky discloses the passwords (gesture pins) are generated during an enrollment session of a new user to obtain access to a secured service/facility (col. 17, lines 5-7). This suggests generating a virtual key of a new user during enrollment is when an initiating event occurs and is detected. Further, Kanevsky discloses the remote transactions between a user and a computer for the computer to classify, identify, and verify the individuals. Kanevsky suggests different requirements for the procedures where individuals must be differentiated so that each command provided to the computer is associated to a particular individual (col. 1, lines 26-27 and 49-57). Kanevsky discloses the gesture pin is transmitted to the user (col. 17, lines 6-7) for use to access the facility/service prompting checking the validity of the gesture pin against the stored ones of a database (col. 15, lines 41-47 and 18, lines 8-24). Thus, Kanevsky suggests defining at least one initiating event for the procedure that does not involve a person arriving at the building and the generated/produced gesture pin is transmitted to the user (col. 17, lines 6-7) suggests generating the virtual key based on the security requirement prior to the person arriving at the building.

Independent Claims 1 and 31 recites initiating event for the procedure and requirement for the procedure. Although, the specification gives examples of the initiating event for a procedure and requirement for the procedure, these terms can be given a broader scope because the specification do not define according to its ordinary meaning. Process Control Corp. v. HydReclaim Corp., 190 F.3d 1350, 1357, 52 USPQ2d 1029, 1033 (Fed. Cir. 1999). For instance, an initiating event for a procedure may be interpreted as a person requesting access, attempting to enter a facility or service, stepping up to a camera, or a motion to trigger a starting verification process. Applicant argues that the requirements are specified in the specification for the key such as security and availability. However, the claim 1 does not limit the requirement for the procedure is based on security or availability. The ordinary meaning according to a dictionary for the term requirement is something required, wanted or needed or a condition. Based on the

ordinary meaning, the claimed defining a requirement for a procedure can broadly be interpreted as to identify or classify what is necessary or a condition (i.e. person with red hair, blue eyes) for access and the claimed generating a key based on the requirement detecting the occurrence of the at least one initiating event can broadly be interpreted as a password or pin produced upon a condition (i.e. person with red hair, blue eyes) of a detected attempt to access a facility or service. Claim 31 recites defining a security requirement and availability requirement for a procedure where this can broadly be given as accessing a facility or service requires secure access (i.e. encryption, password, code, etc.) and what is the available condition for access.

A virtual key (a password, pin, code, etc.) is generated only when the initiating event occurs and is detected broadly suggest the key is produced/given in the first initial process where the system does not know or have the person registered yet which must be during registration/enrollment process. Thus, the key is a newly generated key to be given by the user in attempt to access the facility/service that would be validated to the registration/enrollment key (pre-stored keys) or against keys stored in the database.

An, et al. is brought forth to teach a virtual key can also be considered as a password. An teaches organizations controls access for customers or users by registering user identification and passwords and the password is a virtual key that authenticates a user (col. 1, lines 43-48 and col. 2, lines 4-10). Thus, it would have been obvious for a person of ordinary skills in the art combine Kanevsky and An to teach a virtual key refers to a password (gesture pin) because both virtual keys and passwords has a common function which is for use to authenticate/authorize a user to allow access to facilities/services (An - col. 1, lines 43-48 and col. 2, lines 4-10).

Applicants' Response:

Applicants amended Claims 1 and 31 to clarify that the "at least one person" does not define the at least one initiating event and does not cause the occurrence of the at least one initiating event. Support for the amendments is found in the specification at: Page 3, Lines 22-25; Page 4, Lines 5-9; and Page 6, Lines 1-8.

The method according to the present invention generates a virtual key in response to the detection of the occurrence of a certain event. (Page 2, Lines 22-23) The person to whom the

key is communicated is made to depend on the type of event. (Page 3, Lines 1-2) The event can be an emergency call, an order, a request such as for a cleaning service, an invitation, or a periodically recurring event such as, for example, monitoring a condition, or a service. (Page 3, Lines 23-25) The type of event determines what requirements are specified for the key such as security and availability. (Page 3, Lines 26 to Page 4, Line 3)

It is through the event that the person to be authorized is defined. (Page 4, Line 5) The person is defined in a processing step "Specify Person to be Authorized" **13**. (Page 4, Lines 8-9) As shown in the drawing of the flowchart for the method according to the present invention, the event occurs at the starting point **11** which is before the step **13** of specifying the person to be authorized.

Thus, Claims 21-31 define a method in which the virtual key is generated only when the initiating event occurs and is detected. Only then is the virtual key generated and transmitted to an authorized person. Therefore, Claims 21-31 define a method whereby an authorized person can only access a building if the initiating event has indeed occurred. Examples, of such initiating events are set forth on page 3 of Applicants' specification at lines 23-25.

Applicants' amended step d. of Claims 21 and 31 recites "detecting the occurrence of the at least one initiating event wherein the at least one person does not define the at least one initiating event and does not cause the occurrence of the at least one initiating event".

According to the Examiner, in Kanevsky the claimed defining an initiating even that does not involve a person arriving at the building can broadly interpret as classifying or identifying an event occurring remotely such as a service via the Internet or to another computer of different location. Kanevsky discloses performing a certain act such as access to a service or a facility refers to an initiating event for the procedure (col. 12, lines 42-45) where access to a service can obviously be the initiating event that does not involve a person arriving at the building and remote transactions between a user and a computer (col. 1, lines 26-27).]

Applicants believe that the amendments to Claims 1 and 31 distinguishes the claimed method from the Kanevsky patent that shows a method and a system for user recognition employing behavioral passwords to access a computer, a service, or a facility based upon the initiating event being the presence of a computer user.

In view of the amendments to the claims and the above arguments, Applicants believe that the claims of record now define patentable subject matter over the art of record. Accordingly, an early Notice of Allowance is respectfully requested.